(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11817 A3

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US00/21414

(22) International Filing Date: 7 August 2000 (07.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/147,944	6 August 1999 (06.08.1999)	US
60/148,624	12 August 1999 (12.08.1999)	US
09/632,716	4 August 2000 (04.08.2000)	US

(71) Applicant: SARNOFF CORPORATION [US/US]; 201 Washington Road, CN 5300, Princeton, NJ 08543 (US).

(72) Inventor: WALDMAN, Harvey; 947 Pickering Drive, Yardley, PA 19067 (US).

(74) Agents: MOSER, Raymond, R., Jr et al.; Thomason, Moser & Patterson, LLP, 1st Floor, 595 Shrewsbury Avenue, Shrewsbury, NJ 07702 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

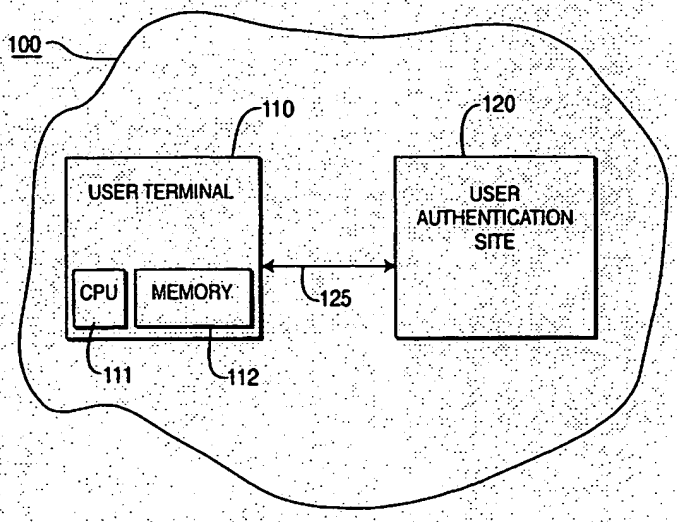
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
6 December 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK USER AUTHENTICATION PROTOCOL



(57) Abstract: In a network having a plurality of user terminals and a user authentication site, a method for authenticating a user. A user terminal of the network receives a password from a user, and translates the password into an authentication encryption key for the user. The terminal generates a first random number, encrypts the first random number with the authentication encryption key to provide a first encrypted message, and transmits the first encrypted message to the user authentication site. The user authentication site decrypts the encrypted first message to provide the first random number, and generates a second random number, which is transmitted to the user terminal. The user terminal combines and encrypts the first and second random numbers, with the authentication encryption key, to provide a second encrypted message. The user terminal transmits the second encrypted message to the user authentication site, which decrypts the encrypted second message to provide the combined first and second random numbers. The user authentication site verifies that the first and second random numbers are correct, and authenticates the user in accordance with this verification.

WO 01/11817 A3

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 00/21414

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KWON T ET AL: "AUTHENTICATED KEY EXCHANGE PROTOCOLS RESISTANT TO PASSWORD GUESSING ATTACKS" IEE PROCEEDINGS: COMMUNICATIONS,INSTITUTION OF ELECTRICAL ENGINEERS,GB, vol. 145, no. 5, October 1998 (1998-10), pages 304-308, XP000793271 ISSN: 1350-2425 abstract page 304, left-hand column, line 1 -right-hand column, line 3 page 306, right-hand column, line 34 - line 60 --- -/--	1,9

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 May 2001	25/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

Inter nal Application No
PCT/US 00/21414

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BHARGHAVAN V: "Secure Wireless LANs" 2ND ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2 November 1994 (1994-11-02), XP002155490 abstract page 11, left-hand column, line 42 -page 12, left-hand column, line 8	1-9